

# Homeland Defense Journal

"He is best secure from dangers who is on his guard even when he seems safe." —Syrus Publilius

Homeland Defense Journal, Inc. | Suite 1003 | 4301 Wilson Boulevard | Arlington, Virginia 22203  
[www.homelanddefensejournal.com](http://www.homelanddefensejournal.com) | Phone: 703-807-2758 | Fax: 703-807-2758

## WHAT'S INSIDE

Capitol Hill Highlights	Page 1
Protecting Information – A Crucial Defense Component	Page 1
Publisher's Notes	Page 2
What They're Saying On The Hill	Page 4
Planning America's Capital with Geographic Information System	Page 8
Calendar of Events	Page 12
Free Space Optics in Homeland Defense and Disaster Recovery	Page 14
The Texas Health Alert Network	Page 17
Envisioning a New Emergency Alert System	Page 20
Five Dos and Dont's of Grantseeking	Page 22
Faces In The Crowd	Page 23
Around the States	Page 25
Homeland Defense Business Opportunities	Page 27
Business Briefs	Page 29

## OUR STAFF

### PUBLISHER

**Don Dickson**  
 ddickson@homelanddefensejournal.com  
 301-455-5633

### EDITOR

**Marianne Dunn**  
 mdunn@homelanddefensejournal.com  
 703-807-2495

### CIRCULATION

**David Dickson**  
 dicksond@homelanddefensejournal.com  
 703-807-2758

### REPORTING STAFF

**Steve Kingsley**  
 skingsley@homelanddefensejournal.com  
 703-807-2758

**Kelly Kingsley**  
 kkingsley@homelanddefensejournal.com  
 703-807-2758

**George Groesbeck**  
 ggroesbeck@marketaccess.com  
 941-360-3663

**Tony Rahimi**  
 trahimi@homelanddefensejournal.com  
 703-807-2758

### GRAPHIC DESIGN

**Dawn Woelfle**  
 dwnmrie@graphic-designer.com  
 941-746-4923

### ADVERTISING AND SPONSOR SALES

**Cara Lombardi**  
 clombardi@homelanddefensejournal.com  
 703-807-2743

## Capitol Hill Highlights

### Congressional actions impacting homeland defense

By Steve Kingsley  
*Homeland Defense Journal*

President Bush requested additional federal funds to cover a shortfall experienced by the Department of Defense, Department of Transportation, FEMA and other agencies facing larger-than-expected costs for homeland defense and national security programs.

Just prior to the Memorial Day recess, the House passed a supplemental funding bill that would provide \$28.8 billion in additional funds for the War on Terrorism and homeland security programs. The Senate is expected to consid-

er the bill sometime during the week of June 3. Its version would provide even more additional funding — \$31 billion — than the House version. The President originally requested \$27.1 billion and has threatened to veto the bill if it goes over that mark.

Expect Congress and the White House to sort this out in late June.

### Bio-Terrorism Bill Clears Congress

Under provisions of HR. 3448, which cleared Congress just before Memorial Day and is awaiting the president's signature, government agencies would receive additional assistance

to prepare for bioterrorist attacks. The bill provides for:

- Authorization of \$1.15 billion for the Department of Health and Human Services to expand stockpiles of key vaccines and medicines.
- Centers for Disease Control and Prevention to receive \$300 million for upgrading facilities.
- Grants to state and local governments to improve planning and preparedness for bioterrorism incidents and public health emergencies.
- HHS to establish a national database of dangerous biological

*continued on page 3*

## Protecting Information – A Crucial Defense Component

By Kem Clawson  
*Homeland Defense Journal*

Homeland defense is more than the protection of bridges, buildings and borders. It also involves safeguarding the lifeblood of our government and economy — information. Without information security, telecommunications, power distribution, public health, national defense, law enforcement and vital government services are at risk.

Although information security has always been important, recent events have underscored the seriousness and scope of the threats against federal, state and local institutions. Attacks could cripple the ability to deploy military and law enforcement resources, maintain vital services or even issue drivers licenses and collect taxes. At the same time, security and other reviews have highlighted gaps and weaknesses in capabilities to protect computers, communications and data. To address these

shortcomings, government units must take immediate steps to identify information security threats, protect IT resources and ensure recovery.

Information security consists of ongoing efforts to protect the transmission, integrity and storage of information from internal and external threats. These threats can range from physical attacks and natural disasters to viruses and worms, hostile intelligence gathering and even biological attack. Protection must cover data and applications, networks, equipment, facilities and especially IT and other personnel. It must also extend across governmental units and contractors.

Both the private and public sectors are now emphasizing information security. However, information security in the public sector is complicated both by the ramifications of an attack, as well as tremendously disparate

*continued on page 6*

# Publisher's Notes

By Don Dickson  
Homeland Defense Journal

Everyone refers to June as the beginning of the lazy days of summer. But they are anything but laid back for the people who work in the homeland defense arena. And Homeland Defense Journal is no exception. We are hosting two conferences this month: Grants Conference Tuesday, June 18 and Homeland Defense Outlook Thursday, June 27.

The Homeland Defense Grants Conference features experts from industry (Grants Co.), government (state of Pennsylvania, as well as guests from federal agencies), and Steve Kingsley, Homeland Defense Journal's writer who covers Capitol Hill. The goal is to bring together key executives from federal agencies (grantors), state and local gov-

ernments (grantees) and suppliers of products and services to this community. For many, this will be the first opportunity to meet and discuss needs, plans and process.

A week later, we'll host the Homeland Defense Outlook Conference. Speakers will shed light funding sources and their outlooks, new products on the drawing boards and in development, special needs and requirements for outfitting, new initiatives at federal, state and local levels, the role of grants in funding local needs and civil agency organization and planning.

Both conferences include breakfast, refreshment and lunch, as well as time to network with agency and industry leaders. We hope you will join us for at least one of these very important and informative conferences. To learn more about them, visit [www.homelanddefensejournal.com](http://www.homelanddefensejournal.com).

*You can go to pages 9 and 15 in this issue for more details.*

## Safety & Security Solutions

- Interoperable Communications & Information Networks
- Identification & Tracking Systems
- Command & Control Operations
- Physical Security & Monitoring Systems

**To Meet Your Needs for Homeland Defense**

[www.motorola.com/homelandsecurity](http://www.motorola.com/homelandsecurity)


**MOTOROLA**  
*intelligence everywhere™*



Information Technology Research Associates Proudly Presents:

## Meeting IT Security Benchmarks Through Effective IT Audits

Learn the Tricks and Techniques Necessary  
to Performing Comprehensive Security Audits  
To Safeguard Your IT Systems

August 8-9, 2002

The American Management Association  
Washington, D.C.

**Join CISSP and CISA-  
certified IT security audit  
practitioners and experts  
to address:**

- IT security audit best practices
- In-house audits vs. outsourcing – pros/cons
- Developing a strategic security audit plan
- Contemporary vulnerability assessment tools and techniques

**Register Today! Call 800-280-8440 or Visit [www.frallc.com](http://www.frallc.com)**

## GIS for Managing the Homeland Security Efforts



A buoyant gas plume model defines simulated contaminated areas around the U.S. Capitol (data courtesy of Vexcel Corporation and Flow Analysis, Inc.).



**ESRI** The GIS Company

E-mail: [info@esri.com](mailto:info@esri.com)

[www.esri.com/homelandsecurity](http://www.esri.com/homelandsecurity)

### Protecting Communities with GIS

Location-based information is crucial to homeland security. Managers at all levels of government must effectively collect, analyze, and share spatial data. Fire, police, public works, public health, building and safety, water, engineering, utilities, and other disciplines utilize geographic information system (GIS) software for analysis and planning; this can be extended to managing and reducing the consequences of all forms of public emergencies.

A primary responsibility of any government is to provide safety and security for its citizens, communities, and assets. GIS is already used in disaster response and can be readily adapted to new homeland security initiatives. For more information on mapping analysis tools, contact one of our homeland security experts today at 1-888-603-3204.

#### GIS aids homeland security efforts in the following ways:

- Improving response capabilities
- Identifying mitigation requirements
- Locating resources
- Assessing community risks
- Developing training scenarios
- Providing timely decision support
- Developing contingency plans
- Managing field data in real time
- Improving data sharing capabilities

Copyright © 2002 ESRI. All rights reserved. The ESRI globe logo, ESRI, ArcMap, ArcInfo, www.esri.com, and @esri.com are trademarks, registered trademarks, or service marks of ESRI in the United States, the European Community, or certain other jurisdictions. Other companies and products mentioned herein are trademarks or registered trademarks of their respective trademark owners.

## Capitol Hill Highlights

*continued from page 1*

- agents and toxins.
- The Food and Drug Administration to increase inspections of food coming into U.S. ports.
- All facilities that manufacture, process or package food (excluding farms) to register with the FDA.
- Vulnerability assessments of water supplies required for all systems that serve more than 3,330 individuals.

### House Passes Customs Border Security Act

The House passed legislation authorizing \$1.4 billion for U.S. Customs programs in fiscal year 2003. Homeland defense activities included in the measure are:

- Deployment of equipment to detect drugs and dangerous materials at ports of entry (\$90 million is authorized).
- Commercial carriers must electronically file a manifest including names of all passengers and crews before entering the country. This includes land, air and water carriers.

Customs must share this information with other agencies.

- Customs will work with the U.S. Postal Service to develop procedures to inspect outbound U.S. mail. However, reading of mail is still not authorized without a search warrant.

### President Signs Border Security Bill

Under legislation signed into law by Bush, the Immigration and Naturalization Service is authorized to hire 2,000 inspectors and investigators over the next five years. The INS would also receive an additional \$150 million for technology upgrades, including electronic scanners for travel documents, at ports of entry.

Schools that admit foreign students must report student participation to the INS.

A comprehensive database will be established to allow the government access to backgrounds of people trying to enter the United States. This database would include names of suspected terrorists and other information from FBI and federal agency databases.

The State Department is mandated to include biometric identifiers on all visas by October 2004.

### Department of Homeland Security Legislation Gets Senate Push

A key Senate committee approved legislation that would create a Department of Homeland Security, thus ending the "grace period" the Senate gave the president to prove that Tom Ridge's Office of Homeland Security could be successful. The bill has bipartisan support, headed by



Sen. Joe Lieberman

chairman Sen. Joe Lieberman, D-Conn., and Sen. Arlen Specter, R-Pa. Homeland security responsibilities of several federal agencies would be combined under this new department headed by a

*continued on page 4*

## Capitol Hill Highlights

*continued from page 3*

secretary of homeland security who would be confirmed by the Senate.

The bill faces a tough road, as the turf battles between involved agencies will be intense. However, the White House has hinted that current Director of Homeland Security, Tom Ridge, may need more statutory authority and may eventually support a watered down version of the bill. The White House is currently engaged in an inter-



*Sen. Arlen Specter*

nal study of the needs of the Office of Homeland Security.

Under the Lieberman bill, FEMA, Coast Guard, Customs and the enforcement activities of the INS would be combined under this new department. However, the FBI and CIA would remain unchanged.

The bill also would create the White House Office for Combating Terrorism. The director of this office, who would be subjected to Senate confirmation, would work with the new secretary to develop a comprehensive counterterrorism plan.

# What They're Saying On The Hill

*By Kelly Kingsley - Homeland Defense Journal*

**Homeland Defense Journal** tapped into the database of its partner, Market\*Access International, to compile these highlights from recent Capitol Hill testimony pertaining to homeland defense.

**Donald H. Rumsfeld,**  
Secretary of  
Defense  
*U.S. Senate  
Appropriations  
Committee*  
Tuesday, May 21,  
2002



Secretary of Defense, Donald H. Rumsfeld, said President Bush requested a \$14 billion supplement for the Department of Defense in fiscal year 2002 and \$379 billion for fiscal year 2003. The 2003 fund would include \$19.4 billion for the War on Terrorism, \$9.4 bil-

lion for war-related programs, and \$10 billion for a fund that would provide for the flexibility needed to respond quickly to changes in operations as the war unfolds, such as:

- Mobilization costs — includes pay for mobilized National Guard and Reserve members who are providing essential support to the War on Terrorism.
- Protecting of military bases and homeland defense — \$8 billion would be directed toward homeland defense programs, totaling \$45.8 billion over the five-year Future Years Defense Program (2003-2007). This is an increase of 47 percent.
- Leveraging Information Technology — \$2.5 billion for programs that leverage advances in information technology to connect U.S. forces in the air, sea and ground. This would total \$18.6 billion over a five-year period, an increase of 125 percent.

Rumsfeld said during the next five years, DoD proposes to invest more than \$136 billion in transformational technologies and systems. Of this, \$76 billion would represent new investments to accelerate or start new transformation programs.

**Keith Rhodes, Chief Technologist,**  
U.S. General Accounting Office  
*U.S. House of Representatives  
Committee on Government Reform  
Subcommittee on Technology and  
Procurement Policy*  
Thursday, April 25, 2002

Keith Rhodes, chief technologist with the U.S. General Accounting Office, addressed a hearing on security technologies to protect federal facilities. He discussed commercially available security technologies ranging from turnstiles, to smart cards and biometric

*continued on page 5*

### ABOUT COBALT

Cobalt is an Internet application development and hosting firm that specializes in working with mid-sized to large corporations and professional trade associations.

For more information go to  
<http://www.cobalt.net/>



### OUR JOB IS EASY...

**WE ONLY HAVE TWO CUSTOMERS\*!**

WE DELIVER -  
DOCUMENT CONVERSION  
OFFICE DOCUMENT SOLUTIONS  
COPIER/PRINTER PROCUREMENT & MANAGEMENT  
\*TO ALL FEDERAL EXECUTIVE AGENCIES  
AND THE DEPARTMENT OF DEFENSE  
SINCE 1949

Visit [www.daps.dla.mil](http://www.daps.dla.mil)  
or call Toll-Free 1-877-DAPS-CAN



CAN DO RIGHT NOW

## What They're Saying on the Hill

*continued from page 4*

systems that could be deployed to protect facilities. He said that while many of these technologies could provide highly effective technical controls, the overall security of a federal building would hinge on establishing robust risk-management processes.

GSA, through the public building service (PBS), owns or leases 39 percent of the federal government's office space and is the primary property manager for the federal government. Within PBS, the federal protective service is responsible for the security of most GSA-managed buildings.

Rhodes said a review performed in April and May 2000 exposed significant security vulnerability in the access controls at many government buildings. He noted that the first line of security within a federal building is controlled entry points where identity verification devices could be used for screening.

He said detection systems provided a second layer of security. Portal metal detectors could be strategically deployed at entry control points to screen individuals for hidden firearms and other potentially injurious objects. Explosive trace detectors, he said, could provide an additional layer of building security.

Although the newer technologies could contribute significantly to enhancing building security, Rhodes said it is important to realize that deploying them will not automatically eliminate all risks.

**Sen. Robert C. Byrd, D-W.Va.**

*U.S. Senate  
Committee on  
Appropriations  
Tuesday, May 7,  
2002*



Sen. Robert C. Byrd, D-W.Va., said the committee needs a better understanding of the military's ultimate goals, more specifics about the plans and objectives and a better explanation as to the duration and scope of various missions. He said the committee also needs more information on how previously approved funding

was spent and added that it should not endorse a blank check for yet-to-be-determined military operations.

Byrd said the nation's effort to combat terrorism is a multi-faceted challenge and that leaders must be realistic about what is achievable. He suggested crafting a responsible spending plan for the Defense Department, and urged members to remain skeptical of any military plan that lacks specific goals, objectives and benchmarks for success.

**Rep. Tom Davis, R-Va.**

*U.S. House of  
Representatives  
Government  
Reform  
Committee  
Subcommittee on  
Technology and  
Procurement  
Policy*



*Friday, May 10, 2002*

Rep. Tom Davis, R-Va., addressed the oversight hearing on intellectual property and government procurement of research and development. He said acquisition legislation in the 1990s streamlined and improved the contracting process. Unfortunately, he noted, 92 percent of the Fortune 500 industries do little or no research and development for the government. He cited a Wall Street Journal article that found that three-fourths of the country's top 75 information technology companies refuse to do this research because of intellectual property red tape.

Davis said that while agencies continue to find companies that will do research and development without intellectual property negotiations, the government must question why leading edge innovative companies refuse to participate.

Davis also noted that research and development would play a critical role in the nation's ability to generate the new ideas and innovation needed to win the War on Terrorism. Technology now accounts for 50 percent of the nation's long-term growth

**Gen. Richard B. Myers,  
Chairman of the  
Joint Chiefs of  
Staff**

*U.S. Senate  
Appropriations  
Committee  
Subcommittee on  
Defense*



Gen. Richard B. Myers, Chairman of the Joint Chiefs of Staff, told the committee that the United States is engaged in the first phase of the global War on Terrorism. He noted that the objectives are clear: Disrupt and destroy global terrorist organizations, eliminate safe havens for terrorists, prevent terrorist access to weapons of mass destruction.

The more that Americans rely on information resources and systems, he added, the greater the efforts must be to protect them. An important step would be the development of military doctrine for information assurance/computer net-

*continued on page 6*

### Seasoned Professionals ... Trusted Advisers

Consulting, sales and  
marketing services

Helping Government  
and Industry  
Succeed in the  
Emerging  
Homeland Defense  
Marketplace.

For information on how  
Market\*Access can assist your  
organization, contact  
Donna Anderson,  
Vice President, at  
danderson@marketaccess.org  
or 703-807-2740.

**Market\*Access**  
International

## What They're Saying on the Hill

*continued from page 5*

work defense. This doctrine, he said, would guide actions in employing safeguards against attacks upon critical information networks.

Myers said the war also has validated the emphasis on the importance of interagency coordination and cooperation, especially the need for close partnerships with domestic and international law enforcement agencies. On the domestic front, he said, the military usually acts in support of civilian law enforcement and first responders, as has been the case in Operation Noble Eagle. He said DoD is building strong ties with

other government agencies in the areas of training, planning, operations and especially in intelligence sharing.

As the war continues, he said, the armed forces will remain focused on the fundamental mission of homeland defense. To better organize forces at home and provide support to civil authorities, the Joint Chiefs modified the Unified Command Plan to establish a combatant command responsible for homeland security. They are also analyzing the potential advantages of combining U.S. Space Command and U.S. Strategic Command into a single organi-

zation. He said they anticipate making a recommendation to the president within the next several months.

Myers said the new Northern Command (NORTHCOM) would help eliminate the seams between the multiple military organizations that share responsibility for homeland defense. It would encompass the continental United States, Alaska, Canada, Mexico and adjoining waters to approximately 500 nautical miles. He said the command would serve as a single point of contact for support to civil authorities and cooperation with North American allies.

## Protecting Information – A Crucial Defense Component

*continued from page 1*

heterogeneous systems, both within and among government units. While the private sector can limit access, many governmental units are required to provide access to public records. The drive toward intergovernmental and departmental information sharing, especially among law enforcement agencies, also makes it harder to balance access and security.

were resolved. Hostile computer penetrations contributed to shutdowns at a Massachusetts airport and an Arizona dam. Even the Pentagon has been hacked into numerous times.

These weaknesses are widely recognized, and are being addressed on several fronts. A recent article in USA Today reported that U.S. Sen. Jon Kyl, R-Ariz., said, "This [cyberterrorism] threat is growing. It's a big threat, because it is easy to do and can cause great harm."

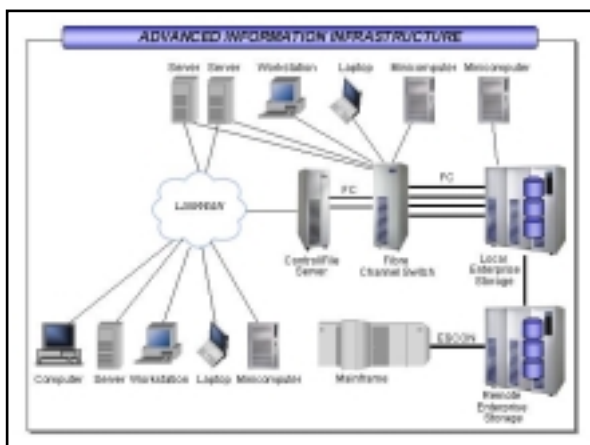
The Bush Administration is seeking about \$4.5 billion, representing about 8 percent of the federal IT budget, to protect computer systems. The National Defense Authorization Act requires agencies to plug information security loopholes. Other congressional legislation, both passed and pending, seek to bolster government information security. The National Association of State CIOs reported that 37 states are developing IT infrastructure protection and disaster recovery initiatives.

In its annual report to Congress, the Office of Management and Budget (OMB) laid out a roadmap for improving information security throughout all government units. The OMB said senior management must pay greater attention to information security. It also recommended improving security education and awareness, upgrading the ability to

detect and share information on vulnerabilities, and ensuring that security criteria are integrated into all investment decisions.

Information superiority — the gathering, analyzing and sharing of relevant information — facilitates the timely and

*continued on page 7*



*Incorporating enterprise storage into an information infrastructure is becoming an increasingly common way to share, protect, and manage information - ensuring survivability and resilience.*

Despite its importance and a \$52 billion federal IT budget, government information security is receiving failing grades. The General Accounting Office (GAO) reviewed computer security deployment at 24 major agencies; 16 received failing grades. A U.S. District Court judge required the Department of the Interior to disconnect its systems from the Internet until security issues



**Disaster Recovery Institute International's** world-renowned professional certification program (ABCP, CBCP, MBCP) acknowledges an individual's effort to achieve a professional level of competence in the industry.

Designed to be rigorous, well controlled, and free of bias, the program is centered on the Professional Practices, our international industry standard. The certification process delivers authoritative recognition of your level of industry knowledge and capabilities.

For more information about Disaster Recovery Institute Certification programs, go to **[www.drii.org](http://www.drii.org)**.

## Protecting Information – A Crucial Defense Component

*continued from page 6*

effective tasking, and deployment of our defense resources. In order to meet these demands, organizations are looking at an information infrastructure to provide a common set of methodologies to manage, protect and share information within an organization. By taking a server-independent view of the information requirements, IT managers are able to architect an infrastructure with a single way to manage the information across a large number of heterogeneous or homogeneous platforms while enabling survivability and resilience. To achieve this, an advanced information infrastructure must have the following attributes:

- **Information Management:** A common information management environment simplifies tasks and provides a centrally managed point of control. For example, it enables seamless backup and restore capability and delivery of user performance data for every platform while driving the standardization of IT processes throughout the enterprise.
- **Information Sharing:** Advanced software intelligence bridges stove-piped mainframe and open systems environments allowing information to be shared without depending upon traditional IP network-based techniques.
- **Information Protection & Survivability:** Enterprise Storage provides reliable mission continuance protection and continuity of operations against planned and unplanned outages through diverse features. This ensures maximum protection and virtually 100 percent data availability.

Together, these attributes can provide the ability to leverage a single infrastructure across the enterprise, resulting in one way of sharing, protecting and managing information. It will help drive standardization to reduce cost, complexity and redundancy without sacrificing the flexibility to support changing business cycles. And through a flexible architecture it has the ability to change and evolve based upon requirements, while eliminating the costly replication of data, equipment, and training.

An advanced information infrastruc-

ture combines common direct and network attached techniques (direct attached storage, storage area networks and network attached storage) in the same architecture to reap the benefits of each connection method. For example, a large Web server farm has two copies of the content that is shared across a NAS connection. When content is to be made available, a script then runs telling the load balancers not to accept new traffic for half of the Web servers while it replaces the old content with the new, and brings the updated servers back online. This process is then repeated for the second half of the servers eliminating duplicate requests and inaccurate data.

This paradigm shift from processor-centric to storage-centric computing provides many benefits critical to information protection. Advanced data storage networking technology can be used to create a heterogeneous storage environment that embodies these attributes and reduces the friction of information access.

One of the key questions asked is "How many copies of information are needed to ensure its survivability?" The answer is in an infrastructure's ability to replicate large quantities of information without impacting production access to the source. Through replication solutions, an infrastructure can function consistently across a wide range of operating environments and databases, at the same time as supporting local and remote wide area replication with minimal bandwidth requirements. Commercial solutions are readily available that provide application independent, differential, remote replication.

While important first steps have been taken to review government information security and address vulnerabilities, more must be done. Information protection must become a part of agency culture and be incorporated into almost every initiative. Some are even recommending that security compliance be a part of every personnel evaluation. Static security policies must be replaced with initiatives that continuously improve — and test — capabilities to protect, mitigate and recover from attacks.

Most important, everyone in government must understand that security is an ongoing process, not a one-time goal. But with the appropriate commitment and expertise, the homeland defense challenge of protecting infrastructure and information can be met — and overcome.

*Kem Clawson is the director of federal technology and strategy at EMC Corp., McLean, Va. He may be reached at (703) 621-1788 or Clawson\_Kem@emc.com*



**Market\*Access Proudly Presents...**  
Government Best Practice Series™  
Training Conferences

Homeland Defense Federal  
Grants Opportunities,  
Arlington, VA – June 18

Homeland Defense  
Budget and Program  
Outlook Conference  
Washington, D.C. – June 27

For details, course agenda and registration information on these important training conferences, go to  
[www.marketaccess.org](http://www.marketaccess.org)

Sponsorships and Homeland Defense Journal advertising opportunities are available.

Contact Cara Lombardi at 703-807-2743

**Market\*Access International, Inc.**  
4301 Wilson Boulevard • Suite 1003  
Arlington, Virginia 22203

Please check our Web site,  
[www.marketaccess.org](http://www.marketaccess.org), for a complete list  
of conference topics, locations and dates.

### Good Design is Good Business

*A freelance graphics studio offering a wide range of computer based design services. From logo design and corporate identity to brochure and press packets, we add versatility, efficiency and professionalism to all your visual marketing needs.*

**Woelfle Graphic Design**

5265D Jamestown Circle  
Bradenton, Florida 34208  
Ph: 941.746.4923 Fax: 425.920.8601  
email: dwnmrie@graphic-designer.com

# Planning America's Capital with Geographic Information Systems

By Michael Sherman and  
Marybeth Murphy  
For Homeland Defense Journal

The Lincoln Memorial, the Washington Monument, the Capitol Building — these are just a few of the landmarks that have become such recognizable symbols of Washington, D.C. Preserving the historic integrity of this great city while planning the future needs of the federal government are the responsibilities of the National Capital Planning Commission (NCPC). These are monumental tasks, but ones that are becoming more efficient with the help of Geographic Information Systems.

Geographic Information Systems (GIS) is a computer technology that integrates mapping with databases hold-

ing various kinds of information, such as zoning, property ownership and utility services. Thanks to a unique federal, local and private-sector partnership, images of Washington's streets, buildings, sidewalks and other elements of the built environment are being digitally integrated with information on the sites. For example, using this data, federal and local governments can easily map and manage a wide array of municipal functions. Using GIS, NCPC analyzes the development of new museums, memorials and public buildings; monitors the management of federal facilities; and supports local economic revitalization. NCPC also expects to lend its GIS capabilities to a new endeavor, led by the Metropolitan Washington Council of

*The National Capital Planning Commission is the federal government's planning agency in the District of Columbia and surrounding counties in Maryland and Virginia. The commission provides overall planning direction for federal land and buildings in the region. It also reviews the design of federal construction projects, oversees long-range planning for future development, and monitors capital investment by federal agencies.*

Governments and the D.C. Emergency Management Agency, which will use GIS data to help develop a regional emergency response plan. This project is envisioned as a system that would allow selected users involved with homeland security in the region to access critical information during a catastrophic event. GIS could become a vital tool in managing crises.

## Washington Geographic Information System

Keeping track of where streets, utilities and buildings

are and who owns them is a key task for federal and local governments. Before the revolution of GIS, NCPC produced new paper maps every five years that were shared with the District of Columbia government and served as the basis for essential functions, including the issuance of building permits, maintenance of water and sewer systems, and the tracking of road signs. Getting anything accomplished invariably involved searching paper files at multiple offices. In pursuit of a quicker, more

*continued on page 10*

  
Security Intelligence Solutions  
present:

## Global Security Summit for Transportation Systems & Critical Transport Infrastructure

The definitive event on multi-modal transportation security issues

**Radisson Hotel, Chicago, USA**

**Two-Day Conference: 4th-5th September 2002**

**Pre-Conference Workshops: 3rd September 2002**

- Discover how leading transport operators have reviewed security since 9/11 and how you can use their experiences to help harden your organizations' security procedures
- In just two days, this event will give you numerous opportunities to glean critical information from other transport operators that will help you tighten your transport security procedures immediately
- Share best practices in security across all transportation modes: Rail, Highway, Transit, Air, Sea
- Get the low down on predicting and pre-empting attacks from national level experts on counter-terrorism
- Assess the origins, magnitude and targeting of the threats to help you direct resources at the most vulnerable points of the system.

For full event details please visit our website at  
**[www.wcbf.com/security/6000](http://www.wcbf.com/security/6000)**

**To Register:** Phone Toll Free: (1) 800-959-6549 or (1)-312-466-5774  
E-mail: [register@wcbf.com](mailto:register@wcbf.com) Register on-line: [www.wcbf.com/security/6000](http://www.wcbf.com/security/6000)

**Early Bird Discount:**  
Register before July 30th  
and get 10% off the  
registration fee

# Homeland Defense *Forecast and Outlook*

**Thursday, June 27, 2002**

**Crystal City Hilton**

At Washington National Airport

2399 Jefferson Davis Highway • Arlington, Virginia

Registration: 7:30 a.m.

Program begins: 8:30 a.m. • Wrap-up: 4:15 p.m.  
Continental Breakfast, Refreshments, Lunch included.



## *Learn about:*

- Programs, funding sources and their outlooks • New products on the drawing boards and in development • Special needs and requirements for outfitting • New initiatives at federal, state and local levels
- The role of grants in funding local needs • Civil agency organization and planning
- Legislative initiatives that are expected to determine new programs and funding sources

## *Featured speakers:*

- U.S. Rep. Curt Weldon, R-Pa. • Ronald E. Miller, Assistant Director, Information Technology Services Directorate and Chief Information Officer, Federal Emergency Management Agency
- Peter, LaPorte, Director, D.C. Emergency Management Agency • Col. Robert L. Coxe Jr., Chief Technology Officer and Chief Information Officer (G-6), U.S. Army • Dr. Anna Johnson-Winegar, Deputy Assistant to the Secretary of Defense, Chemical and Biological Defense • Don Dickson, President, Market\*Access International and Publisher of **Homeland Defense Journal** • Steven Kingsley, Vice President, Research and Government Relations, Market\*Access International • And more – for an updated listing, visit [http://www.marketaccess.org/event\\_hd\\_outlook.asp](http://www.marketaccess.org/event_hd_outlook.asp)

## *Who should attend:*

- Federal systems integrators and solutions providers • State and local domestic preparedness teams
- U.S. Civil agencies with charters to support homeland defense • Computer and information systems security infrastructure executives • FBI • Secret service • Capital Police • State Police • National Guard • DoD
- Federal uniformed police and public safety personnel • Specialists in WMD, Chem-Bio, HazMat response
- Public health and medical services • Metropolitan Medical Response Teams • Industry partners assisting federal state and local organizations • Security professionals

*For more information about this event, visit [http://www.marketaccess.org/event\\_hd\\_outlook.asp](http://www.marketaccess.org/event_hd_outlook.asp) or contact Parrish Knight at [pknight@marketaccess.org](mailto:pknight@marketaccess.org) or (703) 807-2748.*

**Homeland Defense Journal**



**Contingency**  
Planning & Management  
ONLINE



Specialized Technical and  
Technology User Services (STATUS)  
(Advanced Technology Solutions)

**STATESIDE ASSOCIATES**  
Gaining competitive advantage and increasing through  
quality information, expert planning and execution.  
that is the manner of state government relations.

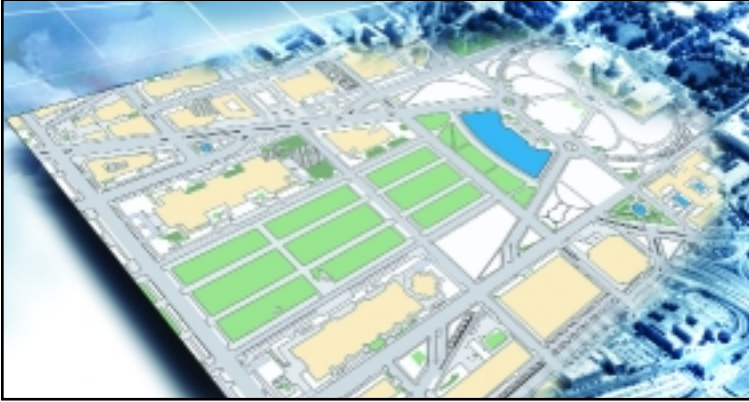


## Planning America's Capital with Geographic Information Systems

*continued from page 8*

accurate means of gathering and integrating data, NCPC sparked a partnership in 1996 between federal, city, regional and private-sector authorities in the development of the Washington Geographic Information System (WGIS).

Working with WGIS partners and customers, NCPC expects to share in the development and use of better planning data and information tools, such as the forecasting of regional population, economics, land use, traffic and transportation; analysis of historic preservation and natural resources; and management of federal facilities.



*Planimetric and orthophotographic data of the National Capital offers diverse applications, ranging from security planning to urban forest cover inventory.*

In the long term, the WGIS partnership expects to enlist the wide participation of the private sector. Such a partnership would support the consortium through the sale and customization of government data. As private-sector partners began to market WGIS data, maps, and images, they found a wide range of interested customers — from architects and developers to realtors and citizens.

The public sector would eventually gain significant financial support for the consortium because of its alliance with private industry. The applications vary and the value of GIS is far-reaching. The Department of State uses GIS to manage its facilities and plan security. The Metropolitan Washington Police Department speeds emergency response times with the help of GIS. The American Forest Foundation uses the system to map and analyze urban forest cover in the national capital region. And the Casey Tree Endowment Fund uses GIS data and standards to inventory street trees, initiating one of the largest urban refore-

The WGIS partnership is a collaborative endeavor that continues to grow in number and in variation. The following list reflects current WGIS partners from federal and District of Columbia governments and the private sector.

### **Federal**

National Capital Planning Commission  
Department of Justice  
General Services Administration  
U.S. Geological Survey  
National Park Service (pending completion of partnership agreement)  
Department of Housing and Urban Development (pending completion of partnership agreement)  
Justice Department  
Centers for Disease Control and Prevention  
Alcohol, Tobacco and Firearms  
Architect of the Capitol

### **District**

Department of Administrative Services  
Department of Consumer and Regulatory Affairs  
Department of Public Works  
Metropolitan Police Department  
Office of Planning  
Office of the Chief Financial Officer  
Office of the Chief Technology Officer

### **Non-Governmental**

Casey Tree Endowment Fund  
American Forest  
George Mason University  
University of the District of Columbia  
Howard University  
D.C. Agenda  
Downtown Business Improvement District  
ESRI Inc.  
The Millennium Institute  
Institute for Defense Analysis  
PEPCO  
Foundation for Educational Innovation  
Metropolitan Washington Council of Governments

estation efforts in the country. Along similar lines, the National Capital Planning Commission has been working with the National Park Service and the Washington Metropolitan Council of Governments to develop a region wide urban forest map. All of these applications are improving the way the private and public sectors conduct business and serve American citizens.

### **About Stateside Associates:**

Stateside Associates helps companies, industry associations and other clients work effectively with state and local governments.

Established in 1988,

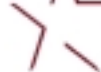
Stateside is the

leading national state

and local government

relations management firm.

## STATESIDE ASSOCIATES



Gaining competitive advantage and cost-saving through quality information, expert planning and execution—that is the essence of state government relations.

The firm's capabilities, depth of experience, dedication to client service and reputation for innovation in government affairs are unmatched. For more information on how Stateside Associates can help your organization, go to [www.stateside.com](http://www.stateside.com).

### **GIS Applications at NCPC**

The National Capital Planning Commission reviews federal development projects in the region, but it also prepares long-range and comprehensive plans for the nation's capital. In 1997, NCPC released "Extending the Legacy: Planning America's Capital for the 21st Century" to guide development in Washington's Monumental Core for the next 50 to 100 years. Preserving the open

*continued on page 11*

## Planning America's Capital with Geographic Information Systems

*continued from page 10*

space and historic vistas in the heart of Washington's Monumental Core became the cornerstone of the Legacy Plan. A key initiative for achieving this goal was to disperse new memorials and museums to all quadrants of the city.

In its development of a Memorials and Museums Master Plan, NCPC used GIS and CAD technologies to identify new development sites throughout the city — sites that would serve as a catalyst to encourage private and local economic development. Using various types of data, NCPC planners could measure the anticipated economic impact of federal development on the local community. And, equipped with CAD animations, planners could be alerted to potential problems in the early stages of design.

To fulfill the Legacy Plan, NCPC identified certain projects as "first initiatives" that should be carried out as soon as possible. In the blighted South Capitol/M Street Corridor, NCPC mapped the area to assist federal and District officials, private developers and citizen groups to identify development opportunities. The digital maps provide up-to-date information — property ownership, land use, zoning, tax status, environmental conditions, etc. — in one widely available and easy-to-use format. NCPC looks forward to the day when this area, located in the shadow of the Capitol, is reborn as a vibrant urban destination of offices, housing, shops, parks and national attractions.

In developing this vision plan, the National Capital Planning Commission recognized that some plans might be implemented in the near future — some projects are already well advanced — while others may come to fruition in the more distant future. NCPC participates in other types of planning, however, that demand more urgent implementation, such as security design and planning. Security has been a necessary feature in the nation's capital for a long time, but the events of September 11 underscored the need for permanent and well-designed security measures. Street closures and a proliferation of hastily installed, temporary elements, including jersey barriers, guard huts and concrete planters, and increasing traffic congestion adversely affected Washington's historic urban design. To address this problem, the National Capital Planning Commission formed an Interagency Security Task Force in March 2001 and released the report, "Designing for Security in the Nation's Capital," in November 2001. One of the report's key recommendations was the preparation of an urban design and security plan to identify permanent, comprehensive security solutions in the capital. GIS mapping and data are key components of this plan, which is expected to be released in the summer of 2002.

The efficient delivery of public services cannot always be accomplished with labor-intensive, quickly outdated maps and decentralized computing. These old planning tools have been surpassed by

GIS. This improved technology — combined with the cooperation of WGIS partners, who share the information they've worked to collect — would allow federal, local and regional agencies to operate more efficiently. In garnering support for GIS in the national capital region, NCPC seeks to fulfill its highest obligation: to ensure a beautiful capital that reflects America's democratic ideals.

*Michael Sherman is the director of the Office of Technology Development and Application Support at the National Capital Planning Commission.*

*Marybeth Murphy is a writer and editor with the National Capital Planning Commission.*

### Can You Be Sure... that you really have a lock on Your Network Security?



The Deception Tool that is the next step beyond firewalls, and Intrusion Detection Systems. Monitors and records new signatures before other security products know of their existence.



Call (800) 334-1553, option #2  
For more information and a demonstration.



### Tac-ALERT™ 2010

#### Responder/Command Tactical Vest Series



• Allows for standardized storage and retrieval of incident response gear with options for sidearm, PAPER and utility/mask carrier rigged for left or right.

• Enhanced visibility/multi-color, removable I.D. and Title panels along with reflective outlining available for positive "Who's who and who's where?"

Tel: (651) 730-7000  
Toll Free: (800) 777-5630  
Fax: (651) 730-5680

• Federal Contract #: GS-07F-0280K (Bomb Disposal & Chemical Warfare Equipment)

• See below for additional features and general information.

• Restricted sale: available to local state/federal agencies only.

2280 Ventura Drive St. Paul, MN  
55125

<http://www.headlitescorp.com>





## JUNE

### Cutting-Edge High Tech Crime Fighting: Best Practices in Computer Forensics

Monday, June 17 – Tuesday, June 18

*The American Management Association*

440 First Street NW  
Washington, D.C.

For more information, visit [www.frallc.com](http://www.frallc.com).

Faculty — Scott Charney, Abigail Abraham, Glenn Lewis, Amber Schroader, and more — will teach you how to find, collect and preserve digital evidence, as well as present the evidence in court.

### Homeland Defense: Grant Opportunities

Tuesday, June 18  
NRECA Conference Center  
4301 Wilson Blvd.  
Arlington, Va.

For more information, visit [www.marketaccess.org](http://www.marketaccess.org)  
Sponsored by: Homeland Defense Journal, INPUT, Department of Transportation TASC, Wireless Communications Association International, Disaster Recovery Institute International, Stateside Associates, Contingency Planning & Management Magazine, Grants Office.

This conference provides a forum for contractors and state and local entities to learn about federal grants for homeland defense and to meet the agency executives who will set up and administer these funded grant programs. State and local emergency management agencies and federal grants executives have the opportunity to meet

and discuss areas of common interest. Vendors who provide products and services supported by federal grants should attend to learn more about the process and meet with potential clients.

### Homeland Defense: Outlook

Thursday, June 27  
Hyatt Regency  
Crystal City, Va.

For more information, visit [http://www.marketaccess.org/event\\_hd\\_outlook.asp](http://www.marketaccess.org/event_hd_outlook.asp)

Market\*Access will host a briefing for government and industry to address four questions surrounding 9/11 and federal agency missions, organizations, priorities and needs:

1. What has happened inside our government because of our national response to this terrible event?
2. What has remained the same?

3. What changes are coming?
4. What is the outlook and forecast for federal, state and local spending?

Speakers will represent federal, state and local government executives and leaders who will provide government and industry attendees with a report on program status, challenges and outlook.

## JULY

### Biometric Identification: Theory, Algorithms, and Applications

Monday, July 8 – Wednesday, July 10

For more information, visit [www.unex.ucla.edu/short-courses/summer2002/bio\\_id\\_theory\\_su02.htm](http://www.unex.ucla.edu/short-courses/summer2002/bio_id_theory_su02.htm)

The instructors are James Wayman, PhD, director, technical security research center, San Jose State University, and Peter T. Higgins, MS, principal consultant and founder, Higgins & Associates International.

*continued on page 13*

Providing the Federal Government with high-demand enterprise services in the areas of:

Information assurance - KCG services include: vulnerability assessment services, network intrusion detection, firewall design and support, PKI, Virtual Private Networks (VPN) development, anti-virus, disaster recovery, and incident handling

Enterprise operations - KCG services include: Enterprise Management and Planning, Onsite Operational Leadership, Customer Support and Response Planning, Deployment, and Web application development

Supporting Federal government organizations within the Intelligence Community, Department of Defense, and Department of Justice

For more information call  
703-467-2000 x 105



**Building, Operating,  
and Securing the  
Enterprise**

**Submit your events by sending  
a short description,  
less than 75 words, to  
[events@homelanddefensejournal.com](mailto:events@homelanddefensejournal.com)**

**Listings will run as space permits.  
To guarantee placement, contact  
Cara Lombardi at (703) 807-2743  
[clombardi@homelanddefensejournal.com](mailto:clombardi@homelanddefensejournal.com)**




The Only Secure Collaboration Platform  
Network-level Security Over The Web  
Multiple Applications  
Customized and Personalized Views  
Workflow Management -  
Capture Best Practices  
Process Efficiency - Guaranteed!  
The Ability to Manage.  
Anywhere. Anytime. Securely  
Edge, Established 1993  
With Over 40% Cleared Staff  
Turnkey Functionality -  
Take The Schedule And Cost Risks  
OUT of Your Portal Project

Visit Us at: [www.edge-technologies.com](http://www.edge-technologies.com)  
or Call Us at: 703.691.7900 or 888.771.3343

## Contribute to Homeland Defense Journal

**Homeland Defense Journal** was created as a forum for the useful flow of information between the private and public sectors that will positively influence and hasten the development of solutions to homeland security requirements.

We invite government employees at every level of government, military personnel, and industry leaders to use this paper as a voice. **Homeland Defense Journal** highlights strides made within the homeland defense community.

If you're in government, describe new initiatives your department or agency is working on. If you're in an industry providing homeland defense solutions, get the word out about your projects and programs that are securing the homeland. Below are some topics we're featuring in upcoming issues.

Write to [editor@homelanddefensejournal.com](mailto:editor@homelanddefensejournal.com) if you are interested in contributing an article or would like a copy of our writer's guidelines.

### Editorial Calendar

Issue Date	Topic	Deadline
June 19	Physical Security	June 7
July 3	Federal Grants Opportunities	June 21
July 17	First Responders	July 5
July 31	Argi-terrorism	July 19
August 14	Intelligence-Information Sharing	Aug. 2
August 28	Responding to Weapons of Mass Destruction	Aug. 16

## Calendar of Events

*continued from page 12*

### Using Fingerprint-Based Checks in Homeland Defense

*Thursday, July 11 – Friday, July 12, 2002*

For more information, visit [www.unex.ucla.edu/short-courses/summer2002/using\\_fingerprint\\_su02.htm](http://www.unex.ucla.edu/short-courses/summer2002/using_fingerprint_su02.htm)

The instructors are James Wayman, PhD, director, technical security research center, San Jose State University, and Peter T. Higgins, MS, principal consultant and founder, Higgins & Associates International.

### Homeland Defense: Emergency Repones Teams

*Wednesday, July 17*

Site to be announced  
For more information, visit [www.marketaccess.org](http://www.marketaccess.org)

### Robotic Systems Design and Engineering

*July Wednesday, July 24 – Friday, July 26*

For more information, visit [www.unex.ucla.edu/short-courses/summer2002/robotic\\_systems\\_su02.htm](http://www.unex.ucla.edu/short-courses/summer2002/robotic_systems_su02.htm)

The instructors are Eric Baumgartner, PhD, senior engineer and group leader, mechanical and robotics technology group, Jet Propulsion Laboratory, and Terrance L. Huntsberger, PhD, senior member of the technical staff, mechanical and robotics technology group, Jet Propulsion Laboratory.

### The STI Knowledge Center Symposium

*Monday, July 29 – Wednesday, July 31  
Bellagio Hotel  
Las Vegas, N.V.*

For more information, visit [www.STIKnowledge.com/symposium](http://www.STIKnowledge.com/symposium) or call (800) 350-5781.

This is a high-level educational symposium for help desk/call center management

executives that focuses on leadership and building a knowledge center. This symposium includes a government interactive workshop track. Magic Johnson is the guest speaker and there will be an exhibit hall with technology leaders from the help desk/call center industry.

### AUGUST

#### Meeting IT Security Benchmarks through Effective IT Audits

*Thursday, Aug. 8 – Friday, Aug. 9*

*The American Management Association  
Washington, D.C.*

For more information, call (800) 280-8440 or visit [www.frallc.com](http://www.frallc.com)

Presented by Information Technology Research Associates.

Learn the tricks and techniques necessary to perform-

ing comprehensive security audits to safeguard your IT systems. Join CISSP and CISA-certified IT security audit practitioners and experts to address IT security audit best practices, in-house audits vs. outsourcing, developing a strategic security audit plan, and contemporary vulnerability assessment tools and techniques.

### SEPTEMBER

#### Global Security Summit for Transportation Systems and Critical Infrastructure

*Wednesday, Sept. 4 – Thursday, Sept. 5  
Chicago*

For more information, contact Vijay Bijaj at [vijay.bijaj@wcbf.com](mailto:vijay.bijaj@wcbf.com).

This conference will address future challenges facing transport operators in all sectors worldwide in

*continued on page 14*

## Calendar of Events

*continued from page 13*

preventing terrorism by bringing together a panel of leading experts and practitioners in transportation security and terrorism to help the passenger transport industry design more effective countermeasures and develop improved crisis management and emergency planning strategies.

### 2002 Homeland Security and National Defense Symposium

Monday, Sept. 9 - Friday, Sept. 13  
Atlantic City, N.J.

Sponsored by the Fort Monmouth Chapters of Armed Forces Communications Association (AFCEA), Association of Old Crows (AOC) and Association of the United

States Army (AUSA)

For more information contact Frederick W. Eisele at (407) 310-3556 or send an e-mail to fred213@msn.com.

This symposium will present ongoing or planning-stage initiatives at Fort Monmouth to provide information technology and communication packages that are ready to be flown to any part of the northeast whenever

needed by FEMA, the Governor or the National Guard. Other sessions will investigate the roles of agencies in homeland security and the military efforts to combat terrorism. The subject of providing logistics support to military, paramilitary and national law forces also will be examined.

## Free Space Optics in Homeland Defense and Disaster Recovery

By Nagesh Chowla  
For Homeland Defense Journal

The September 11th disaster has been described as a war zone where communications ceased in lower Manhattan. Businesses and government facilities found that they had lost their telephone lines, cell phones, computer systems, software under development and information from employees' desks, as well as much of the ability to provide search and rescue. Free space optics played a vital role in providing emergency services,

government operations and getting the business community back in operation in the days following the devastation.

Free space optics is a reliable, fiber alternative, license-free, quickly installed wireless technology used to transmit data between buildings located up to two and a half miles apart. It has data rates from a million bits per second to more than 1 billion bits per second. One high-capacity link has the ability to carry up to 125,000 simultaneous phone calls. The technology is extensively used in myriad primary communications applications.

### Test and Verify!

### Ethical Hacking Penetration Testing

Only one firm should be  
leaping through your firewall



# TIGER TESTING

The Independent Computer Security Testing Specialists

## Independent Testing Is Better Testing.

**Tiger Testing's independence assures unbiased and complete test results.**

Web site security testing is 100 percent of what we do. We do not sell: auditing, consulting, software, hardware, hosting, firewall, or networking services or products. We have no conflicts of interest. Tiger Testing's GSA Schedule number is: GS-35F-0141L.

30 Wall Street, New York, NY 10005, (212) 898-9385  
[www.TigerTesting.com](http://www.TigerTesting.com), sales@tigertesting.com

### In Action After Sept. 11

The sudden destruction of the World Trade Center buildings, which housed network equipment for all cellular service providers, greatly reduced — and in some cases eliminated — telephone and radio coverage throughout lower Manhattan.

Within 24 hours of the worst terrorist attack on American soil, engineers and technicians were working with cellular telephone companies and the New York Port Authority to re-establish telephone and radio coverage at ground zero. PAV Data, a free space optics manufacturer in England, worked over the weekend following Sept. 11 to manufacture and air freight five free space optics links, each having a 6 million bits per second capacity, which provided the bandwidth for about 480 simultaneous wireless telephone conversations by reconfiguring existing cellular telephone infrastructure in New Jersey.

Increasing cellular coverage in the World Trade Center area helped rescue efforts as trapped people used cell phones to call authorities. Many emergency medical service, police, fire professionals and volunteers used cell phones that communicated over free space optics links to keep in contact with rescue agencies and each other. The free space optics links also assisted family

*continued on page 16*

# Federal Grants for Homeland Defense Programs Training Conference

Another in the Market\*Access Government Best Practices Series™

**Tuesday,  
June 18, 2002**

**NRECA Conference Center**

4301 Wilson Boulevard  
Arlington, Virginia 22203

Registration starts at 7:30 a.m.

Program begins at 8:30 a.m. and wraps up at 5:00 p.m.

Continental Breakfast, Refreshments, Lunch included

**Market\*Access**  
International

Federal domestic funding for homeland security is expected to top \$42 billion in fiscal year 2003. That substantial sum will be routed through not less than 14 federal agencies in the form of at least 45 aid programs. Each congressional appropriation is tied to a specific federal agency charged with the responsibility of disseminating the funding according to the legislation that created the program.

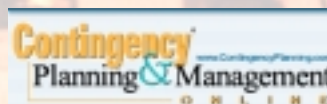
Federal Grants for Homeland Defense Programs Training Conference is a forum for contractors and state and local entities to learn about federal grants for homeland defense. Attend this conference and meet the agency executives who will set up and administer the funded grant programs for homeland defense.

Learn about federal agency plans, programs and new homeland defense initiatives. Find out more about new techniques and practices used for landing homeland defense grants. Listen to the experts talk about their success and lessons learned. Discover new opportunities and management strategies. Pick up tips on e-grants and the grant process.

For more information, including a list of speakers,  
visit the Market\*Access Web site at [www.marketaccess.org](http://www.marketaccess.org) or go directly  
to the event listing at [www.marketaccess.org/event\\_hd\\_grants.asp](http://www.marketaccess.org/event_hd_grants.asp)



**Homeland Defense Journal**



## Free Space Optics in Homeland Defense and Disaster Recovery

*continued from page 14*

members contact those unable to call home due to the overburdened telephone system. Other free space optics links from several manufacturers were installed quickly in lower Manhattan to provide voice and data services to the Federal Emergency Management Agency, the Manhattan courts and a large financial management and advisory company. Many of the links were able to shoot the beams across the Hudson River at a distance of more than one and a half miles at a data rate of a billion bits per second.

### The Technology

Free space optics links communicate through the air by connecting transmitter-receivers or transceivers to each other by using invisible infrared light as a medium between buildings or towers. The electronics used are solid-state semiconductor based and consequently highly reliable. Building transceivers can be mounted on rooftops, balconies, on outside walls or inside windows. Transmission is inherently secure as the optical beam is narrow, further security is provided by coding the signals. Certain networks additionally encrypt the signal for ultimate security.

This optical technology does require that the transceivers are within line of sight of each other. Multiple free space optics systems can be mounted on the same rooftop or tower. The narrow beams prevent interference, unlike microwave links. Free space optics technology is different from radio or microwave in that it does not operate in licensed frequency bands and, consequently, can be installed very quickly as was the case after the World Trade Center disaster. When facilities are moved, equipment is easily moved between installations, as it is light and license-free. Free space optics equipment has been installed in the extreme cold of Siberia to the heat of Saudi Arabia and Egypt.

Transmission errors are specified as less than one bit in 10 billion and often measure less than one error in a trillion bits, comparing favorably with fiber bit error rates. Long-term tests in customer facilities conducted by Telelase Communications have shown near six nines (better than 99.999 percent) avail-

ability although the industry commonly predicts 99.1 percent or better reliability in many applications. Financial payback periods are as low as one and a half months of leased line costs.

Connections for free space optical devices to local networks or carrier networks are as simple as connecting another network device such as a computer, hub or router. Connections to networks commonly use fiber or copper as a physical transmission medium and support Ethernet, fast Ethernet and gigabit Ethernet protocols.

Unlike leased lines that have a monthly service fee, free space optics equipment is normally purchased and there are no monthly recurring charges other than routine maintenance that consists of annual cleanings and infrequent realignment. Internal electronic parts rarely need replacement. The biggest limitation to the use of this technology is that obstacles, such as buildings and trees, in the optical path could block the beam; a clear line of sight is essential.

Additional features of free space optics systems that make them suitable for homeland defense applications are their relatively small size and weight and their ability to operate from batteries and uninterruptible power sources. Many of the systems look similar to security cameras or red light cameras used to photograph traffic violations. This makes the systems aesthetically unobtrusive and able to be mounted in small spaces. The low power consumption and battery operation capability means that when power is interrupted, the links keep operating and can be used to continue uninterrupted life saving voice and data traffic and legally required access to 911.

Products using free space optics technology have been in commercial use for more than a decade and worldwide over 10,000 systems have been installed.

### Homeland Defense and Disaster Planning

The major emphasis of free space optics is greater than a reactive technology for disaster recovery. Its greatest benefits comes from year round use as a short-range, high-bandwidth, cost-effective technology that has low recurring

costs. Systems are commonly used wherever fiber communications is not possible due to land use restrictions, property rights and waterways. Some common uses are cell base station communications to wireless carrier central offices, building to building or intra-campus broadband communications and access to the Internet and carrier circuits. Hospitals use the links to transmit medical data and records. Racecar crews use this to pass data and voice traffic with off-site facilities.

We now get near daily warnings of possible terrorists activity in the United States. Government agencies and commercial organizations need redundant communications technologies to keep vital voice and data services functioning despite the possibility a single resource, building or area cannot be used or is gone. Free space optics should be used redundantly with fiber, wire or radio wherever available all-the-time communications are critical. A viable and cost effective technique is to put high bandwidth traffic on wireless free space optics and back it up with lower bandwidth landlines or microwave radio. After September 11, forward thinking organizations have started to do just that.

*Nagesh Chowla is the chief executive of Telelase Communications Inc. in San Ramon, Calif. The company provides free space optics systems, networking equipment products and engineering services. He can be reached at [nchowla@telelase.com](mailto:nchowla@telelase.com) or (925) 265-4040.*

**SIEMENS**

<http://www.siemensgovt.com/>

A potent mix of cutting-edge speakers and powerful technologies  
One of the world's most technical conferences on computer security

Master the art of...

# digital self defense

*More security ninjas prefer Black Hat than any other brand.*

## sponsors

diamond

BIND VIEW RAZOR

platinum

net INTRUSION

PRICEWATERHOUSECOOPERS

gold

NORTEL NETWORKS

silver

Microsoft SECURE COMPUTING

lead portal

SecurityFocus

Training: 2 days, 10 topics

Briefings: 2 days, 8 tracks, 40 speakers



100% pure information.

## Black Hat Briefings & Training: USA 2002

Training: July 29-30 • Briefings: July 31-August 1 • Caesars Palace, Las Vegas, NV

WWW.BLACKHAT.COM FOR UPDATES AND TO REGISTER OR CALL +1.916.853.8555

## The Texas Health Alert Network

By Michael Mastrangelo  
For Homeland Defense Journal

In the summer of 1999, the Texas Association of Local Health Officials (TALHO) recognized bioterrorism as a viable threat. With federal funds from the Centers for Disease Control and Prevention, supplemented by money from the Texas Telecommunications Infrastructure Board — which uses assessments on telephone service to fund the development of telecommunications infrastructure for schools, nonprofit healthcare facilities, higher education and libraries — the Texas Health Alert Network (Texas HAN) was born.

The Texas HAN is run by local health departments through TALHO. In Texas, local health departments are not affiliated with the state department of health, but are run by local jurisdictions and established under the authority of the Texas Health and Safety Code.

### Obstacles

In 1999, very few people believed that bioterrorism was a credible threat,

making the creation of the network as much a political effort as a technical effort. That summer, TALHO began planning for the Texas HAN with funds from CDC and TIFB.

To date, TIFB has funded approximately \$1 billion in telecommunications projects. Prior to 1999, local health departments were not considered eligible for this type of funding. They could provide primary care and apply for the funds as nonprofit clinics, however, the definition of primary care was elusive.

In July 1999 TALHO — represented by Wayne Farrell, director of the Bell County Public Health District; Bob Galvan, associate dean of the University of North Texas Health Science Center's School of Public Health; and Dr. Christine Bradshaw of Texas Department of Health (now with CDC) — told TIFB that telecommunications technology could play a role in active disease surveillance. The technology also could play a crucial role in the early detection of a covert bioterrorist event. They pointed out that modern and redundant communications links would be needed for the

rapid dissemination of health alerts.

In his article "Toward Biological Security," published in the magazine *Foreign Affairs*, May/June, 2002, National Security Council staffer Christopher Chyba said public health surveillance for signs of unusual disease is critical.

"Improvements in 'sensitivity' and 'connectivity' are required," he noted. "Sensitivity means the recognition by healthcare workers that an illness is out of the ordinary; connectivity is the reporting of this recognition to local, state and national authorities, and consequent timely help with diagnosis and treatment."

Although not immediate, the TIFB ultimately released a special request for proposal to support the Texas HAN. A collaborative of 64 local health departments applied for and received a grant of \$3.78 million. They were able to use the majority of the initial \$744,655 received from the CDC to provide the local match required for TIFB funding. TALHO is now seeking support in Texas to interconnect with many of the existing TIFB-funded networks and telemedicine net-

*continued on page 18*

## The Texas Health Alert Network

*continued from page 17*

works to provide more expansive coverage.

Of the \$51 million of federal funds Texas plans to direct toward bioterrorism preparedness, TALHO would use \$3 million to support recurring line charges for the network and to expand the network to cover more sites. In accepting the federal monies, Texas is obligated to meet the CDC's requirement that Texas HAN cover 90 percent of the population with connectivity to all health departments, hospital emergency rooms and law enforcement agencies.

"If we are successful in internet-working with existed TIFB-funded infrastructure, we will greatly accelerate meeting this goal," said Lee Lane, TALHO executive director.

### The Technology

Texas has 254 counties, so it is highly unlikely that planning and training could happen without the use of modern telecommunications capabilities. The Texas HAN would offer an array of distance learning and conferencing capabilities, which would play a key role in increasing workforce capacity at the local level to detect and respond to bioterrorist events.

Most experimentally established response protocols on the books were based on military experiments conducted decades ago. They were centered on militarily significant results, because there wasn't a wide body of experimental evidence on the specifics for responding to a deliberate biological attack on a large population. But that is now changing, as was apparent with the anthrax attack. During that attack, once-standard advice on the potential for re-aerosolization of anthrax spores wasn't appropriate for the risk to civilian populations.

A great deal of learning is expected to take place during the actual response to an event. And, the newly acquired information on the best response protocols must be rapidly disseminated to responders across the country. The only way to accomplish this is to use modern telecommunication systems.

The backbone of the Texas HAN is a frame relay T-1 network (a T-1 line with 1.54 Mbps bandwidth, which is equivalent

to 24 regular phone lines). The network's enterprise site is located at a state facility and the Texas Department of Public Safety provides physical security. Connectivity is provided by the state public telecommunications backbone, TexAn2000. TexAn200 is run by the Department of Information Resources, which received its initial funding for TexAn from the TIFB.

Private virtual circuits (PVC) attach each endpoint with the enterprise site. In the event of loss of the enterprise site, a fail-over system would provide for PVCs to a backup site approximately one hundred miles away.

The Texas HAN is connected to the state intranet and the Internet via a DS-3 connection, which is equivalent to 672 regular phone lines. Firewalls and intrusion detection devices add to security of the system. Because CDC requires an alternate method of connectivity in case the primary connection goes down, each router at the endpoints has a minimum of two interface cards: one for the dedicated T-1 network and another fail-over connection to an Internet service provider that could be used to establish a virtual private network connection. Plans include additional backup capability at one of the state's disaster recovery operations centers. The initial implementation of the Texas HAN is scheduled for completion June 30, 2002.

To ensure that local health department directors could send and receive health alerts around the clock, a wireless component would be added to the Texas HAN. Each local health department site would eventually have satellite downlink capability, interactive two-way videoconferencing, and a local cache engine for storing streamed video programming.

TALHO also is exploring implementing a system of high frequency radios to provide long distance emergency communications to strategic points in the state and CDC. The system would be selected with ease of use in mind and would allow operators to communicate by using their e-mail client as the interface to the system. Additional voice capability would be provided by using Internet protocol telephony or voice over Internet protocol. Because voice traffic would be carried

over the network, public health officials could collaborate without incurring long-distance charges. The network also would have an audio bridging capability so officials could establish conference calls on demand. Video bridging would be provided by a multipoint control unit.

In some Texas jurisdictions, fax machines are still the preferred method of communication. In those areas, a four-port broadcast fax board is being added to the local area network server. The four ports would connect to four phone lines so that the local director can send broadcast fax alerts to local hospitals, physicians and other first responders.

An important feature of the system is its dual use capability — the equipment and systems would be used in the normal course of public health business, not designated for emergencies only. Although good communications capabilities are essential for a bioterrorism response, the system's real value is its capability to foster disease surveillance and consequence management applications that could be delivered over the network to the officials that need them to assist in decision making.

*Michael J. Mastrangelo is the director of the Texas Health Alert Network Project and a member of the federal advisory committee for data interoperability for weapons of mass destruction response - health services subcommittee for consequence management interoperability services; and a member of the Texas Telecommunications Infrastructure Fund, Health Care Working Group.*

**UNISYS**

<http://www.unisys.com/>

**! ON-SITE POWER GENERATION !**  
**! COMMUNICATION FACILITY DESIGN/BUILD !**  
**! 24 HOUR HIGHLY REDUNDANT**  
**POWER SOLUTIONS !**



**ESI International**

8(a) Certified; Disabled Veteran Owned Business

Offices: Florida, Virginia, Mexico, Brazil

**Infrastructure design and engineering, equipment sales, project management, testing, service and maintenance Generators, UPS, A/C, Chillers, DC plants, surge suppression, batteries 20-year old company; 4 million sq. ft of design/built critical communication and information systems and facilities**

**ESI International Design/Builds Critical Facilities  
and Systems to achieve the highest degree of  
reliability through award winning, innovative,  
cost lowering designs**

**Stan Adwell Director of Sales and Marketing**

**813-740-1421**

**813-781-4146**

**[sadwell@esi-international.com](mailto:sadwell@esi-international.com)**

# Envisioning a New Emergency Alert System

By George Q. Nichols  
For Homeland Defense Journal

Over the past six months, the Partnership for Public Warning (PPW) has pursued its task to improve the nationwide Emergency Alert System. When formation of the public-private partnership was announced in December 2001, some speculated that the alert system was fast becoming obsolete. Since the alert system was established in the Cold War year of 1951, new, innovative technologies of the 21st century could update and add value to the current system.

Some elements of these modern technologies would be incorporated into the new system. However, the backbone of the new system would rely heavily on the most ordinary, yet widely used 20th century communications device – the telephone. Found in nearly every home and office — and now in many pockets and purses — the telephone is the preferred communications medium nationwide.

The ubiquity of this modern-day device, combined with appropriate computer software and an efficient operational structure and protocol(s), could yield a cost-effective system. Implemented nationwide, it would create a functioning notification system within a reasonable timeframe and fulfill the promise of the first emergency broadcast system.

## The Emergency Alert System

The Emergency Alert System (EAS) is the third version of a nationwide public notification system that began in 1951 as

Control of Electronic Radiation (CONELRAD). At the time, defense officials feared Soviet bombers would hone in on targeted cities using commercial radio station signals and attack the United States. The solution was to issue a CONELRAD alert, ceasing normal operation of all radio stations and having select stations broadcast the message on either 604kHz or 1240kHz.

In 1963, with intercontinental ballistic missiles and their sophisticated guidance systems not relying on radio navigation, CONELRAD was deemed obsolete and the Emergency Broadcast System (EBS) was born.

Advances in digital technology finally led to the development of the Emergency Alert System (EAS) in 1997. This system does not rely on a "daisy chain" structure, skips the "alert," and allows information to be broadcast immediately. It can be activated automatically without station personnel, includes cable broadcast systems and uses the same signal as the National Weather Service.

However, none of the alert systems has been used in a major nationwide emergency. Instead, the main use is to issue weather warnings, primarily in the South for tornadoes and along the East Coast for hurricanes.

## Why a new system?

With 24-hour television, radio news stations, e-mail and pagers, a nationwide emergency alert system would seem a relic of a bygone era. However, many situations exist in which people need to be notified immediately, regardless of location. When a tornado strikes a community or terrorist groups threaten public safety, many lives could be saved if people receive timely, accurate information or instruction. The primary role of the EAS is to inform people of a critical situation and encourage them to seek more information from broadcasters or other sources.

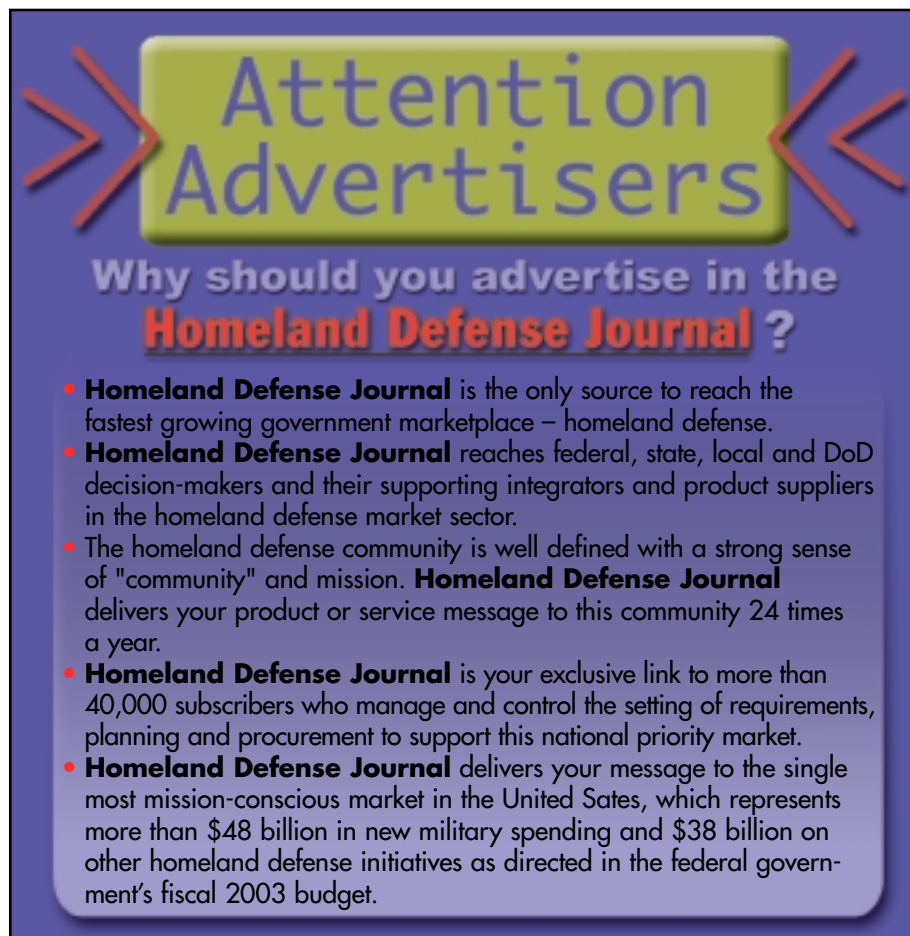
The EAS also allows many state managers to independently trigger emergency warnings to those at risk. Using varying systems and protocols, federal, regional, state/local police, fire, medical response and disaster teams routinely rely on these emergency warnings to aid in public safety initiatives. Often limited by the economic status of these agencies, some still use manual call trees, and others still rely on even more old-fashioned loudspeakers and sirens.

With the nearly simultaneous attacks on Washington, D.C., and New York City, September 11, 2001, in addition to the plane crash in Pennsylvania, the need for a coordinated nationwide exchange of information and issuance of warnings became increasingly evident.

## The Creation of the Partnership for Public Warning

For these and many other reasons, the PPW began bringing together various representatives of the many stakeholders involved in warning systems for the examination of the nation's alert system. Following an initial meeting in November

*continued on page 21*



**Attention Advertisers**

**Why should you advertise in the Homeland Defense Journal?**

- **Homeland Defense Journal** is the only source to reach the fastest growing government marketplace – homeland defense.
- **Homeland Defense Journal** reaches federal, state, local and DoD decision-makers and their supporting integrators and product suppliers in the homeland defense market sector.
- The homeland defense community is well defined with a strong sense of "community" and mission. **Homeland Defense Journal** delivers your product or service message to this community 24 times a year.
- **Homeland Defense Journal** is your exclusive link to more than 40,000 subscribers who manage and control the setting of requirements, planning and procurement to support this national priority market.
- **Homeland Defense Journal** delivers your message to the single most mission-conscious market in the United States, which represents more than \$48 billion in new military spending and \$38 billion on other homeland defense initiatives as directed in the federal government's fiscal 2003 budget.

## Envisioning a New Emergency Alert System

*continued from page 20*

2001, with 125 participants, a 24-member interim board of trustees was created. This board includes individuals from the emergency notification industry; state emergency managers from Alaska and Vermont; academic professionals, consultants and government employees from federal agencies, including the Federal Emergency Management Agency, NASA, National Weather Service, U.S. Geological Survey, National Communications System and the Federal Communications Commission.

A membership organization, the PPW seeks funding and participation from federal, state and local governments; businesses; charitable organizations and others. Since December 2001, the group has met monthly in Washington, D.C., to work with the Office of Homeland Security and federal agencies to clarify roles and responsibilities. The PPW also is also reaching out to numerous other industries and organizations that play a role in emergency warning and response.

"Our goal," said Peter Ward, chairman of the PPW board of trustees, "is to develop consensus on standards, procedures and points of interoperability so that businesses can see opportunities and viable markets for delivering innovative warning systems."

The PPW is organizing a workshop in June 2002 to bring together physical and social scientists with extensive experience in issuing warnings and evaluating their effectiveness. Specialists in terrorism and weapons of mass destruction will attend. The group will recommend ways to improve the Homeland Security Advisory System announced by Tom Ridge, OHS director and former governor of Pennsylvania.

In June, the PPW also will begin a process to develop a national strategic plan for public warning. The first step is to collect information on benefits and problems with current systems, catalog systems available, and recommend those who should help write the strategic plan. To participate, visit the PPW Web site [www.PartnershipForPublicWarning.org](http://www.PartnershipForPublicWarning.org) after June 1, 2001, and download the request for information. A draft will be written this summer.

"In the fall, we hope to travel the country seeking reviews and input so that this plan when released next year, will have widespread support," said Ward.

### Basic Elements of the Plan

From the PPW's first meetings, some initial elements have appeared that are likely to be included in the strategic plan. They include:

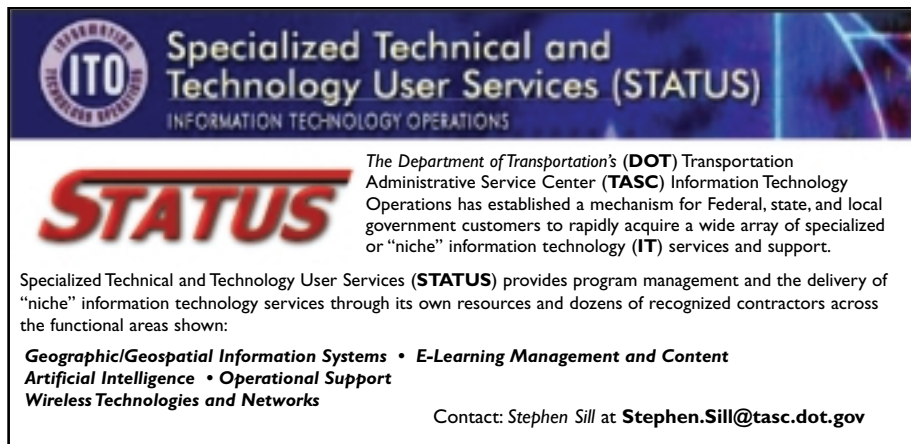
- **National Infrastructure** – While disaster alerting, response and recovery are local issues, a national infrastructure for collecting and distributing warnings is needed. This may require funding from the federal government.
- **Omnipresence** – Warning systems must reach first responders and residents through various communications media. Therefore, receivers need to be contained within widely used products such as telephones, radios, televisions, computers and pagers.
- **Digital Messaging** – As telephones, radios, televisions and handheld devices move into the digital era, warning capability can easily be incorporated after standards are established. Digital messaging using

cellular telephones and other handheld devices worked extremely well during the tragic events of September 11, even though the voice networks were overloaded.

- **Smart Receivers** – EAS warns many people not at risk. Smart receivers know the locations where they are placed and what content applies to their owners. These receivers could scan all warning messages and relay only the appropriate ones. In addition, the message could be sent in one of many languages and in methods appropriate to the individuals receiving it, for example, to people who are visually or hearing impaired.
- **Standards and Procedures** – In many ways, technology is the easiest part of an effective system. Other major needs include training; standard, all-hazard terminology; professional standards; and procedures for issuing warnings reliably and securely from potentially thousands of sources.
- **Bi-directionality** – Many local and regional agencies, as well as corporations that need to summon or notify personnel, use bi-directional communications systems. The PPW plans to examine the potential of incorporating this capability into some national systems for accountability purposes in knowing who is safe or who will be responding.
- **Software** – With numerous existing software solutions that use the basic telephone and computer infrastructure, the PPW would designate the parameters to be met by software providers. Companies would realize an economic incentive to create software that meets these federal standards.

For the PPW, the bottom line is crafting a cost-effective solution that provides timely, accurate information or instruction during times of crisis, nationwide threats or hazardous events of any size, creating a system that would ultimately be flexible enough to withstand inevitable advances in technology and to serve its nation well.

*George Nichols is group vice President at Dialogic Communications Corp. He can be reached at [george.nichols@dccusa](mailto:george.nichols@dccusa) or 781-410-2024.*



**Specialized Technical and Technology User Services (STATUS)**  
INFORMATION TECHNOLOGY OPERATIONS

The Department of Transportation's (DOT) Transportation Administrative Service Center (TASC) Information Technology Operations has established a mechanism for Federal, state, and local government customers to rapidly acquire a wide array of specialized or "niche" information technology (IT) services and support.

**STATUS**

Specialized Technical and Technology User Services (STATUS) provides program management and the delivery of "niche" information technology services through its own resources and dozens of recognized contractors across the functional areas shown:

**Geographic/Geospatial Information Systems • E-Learning Management and Content  
Artificial Intelligence • Operational Support  
Wireless Technologies and Networks**

Contact: Stephen Sill at [Stephen.Sill@tasc.dot.gov](mailto:Stephen.Sill@tasc.dot.gov)

## Seasoned Professionals – Trusted Advisers



**Providing government-wide and agency-specific consulting, marketing and sales services**

- **Opportunity identification • New product launch**
- **Sales and marketing**
- **Capitol Hill – Legislative Liaison**
- **Sales training • Market research**
- **Business planning**

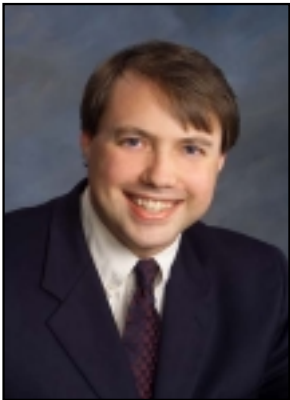
**Assisting industry and government fee-for-service agencies to develop and successfully execute federal business plans.**

### *How can we help you?*

For more information, contact  
Donna Anderson, Vice President  
Market\*Access at 703-807-2740  
or [danderson@marketaccess.org](mailto:danderson@marketaccess.org)

## Five Dos and Dont's of Grantseeking

By Michael Paddock  
For Homeland Defense Journal



1. **Do** research every funding source to which you intend to apply. Nearly every funder, from the very small local foundation to the large government agency, receives many more requests than they can fund. The best way to maximize your effort as a grantseeker is to understand as much as you can about what the funder is interested in supporting. Many government grants will indicate the most important elements of the application by weighting the scores.

2. **Do** tailor each proposal to each funder. Avoid a shotgun approach and try to budget your grantseeking time so that you can review each proposal from the standpoint of the reviewer. Generally, sections that are weighted with a higher score in the application packet should be longer and more detailed than those with a lower weight.

3. **Don't** include any materials in your application other than those specifically requested. Except for small foundations that may not have published proposal guidelines, most funders will detail in the application packet exactly what should be

*Michael Paddock is a featured speaker at Market\*Access International's Federal Grants for Homeland Defense Programs training conference that will be held Tuesday, June 18 at the NRECA Conference Center in Arlington, Va. His presentation, "Bringing Homeland Defense Funding Home," will include five new dos and don'ts and a variety of tips on finding and accessing homeland defense grants and contracts. For more information about the conference, visit [http://www.marketaccess.org/event\\_hd\\_grants.asp](http://www.marketaccess.org/event_hd_grants.asp).*

included. Adding videos or other ancillary materials may weaken your proposal, since these materials are often discarded or (less frequently) returned. If you referred to them in your proposal, they won't be there for reviewers to view. In the worst case, additional materials might disqualify your application entirely.

4. **Do** contact the foundation administrator or grant program staff and attend any bidders' conferences or informational sessions the funders may offer. Many grant programs have a certain "personality," characteristics that are common to all funded projects. The program staff can give you tips on these characteristics and information sessions can give you the insight you'll need to gain a competitive edge. One caveat: certain grant programs discourage applicants from contacting reviewers after the deadline for the applications has passed. Be

*continued on page 23*

## Five Dos and Dont's of Grantseeking

*continued from page 22*

aware of the policies for the funder you're considering contacting so your proposal is not accidentally disqualified.

5. **Do** frame questions to get a meaningful response. Many program staff (particularly for government programs) will not tell you that you can't spend three-fourths of your budget on equipment. They like to leave it to the grantseeker to describe the program and then have reviewers decide whether it fits within the program guidelines. A better way of asking, "can I use three-fourths of my budget for equipment" might be "how much of their budgets have past grantees spent on equipment?"

**Grow**  
your federal IT business

**Develop**  
your federal pipeline

**INPUT** Empower your federal sales and business development team with the industry's most advanced on-line database of federal IT contract opportunities, agency analyses and market assessments.

For a Free Trial visit <http://www.input.com/gov>

<http://www.input.com/gov>

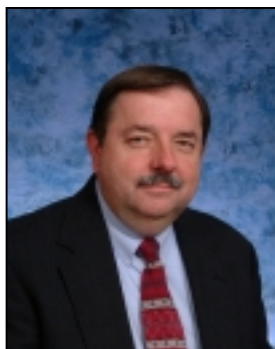


*Michael Paddock is the chief executive officer for Grants Office, LLC. Contact him at [mpaddock@grantsoffice.com](mailto:mpaddock@grantsoffice.com) or visit [www.Grantsoffice.com](http://www.Grantsoffice.com)*

## FACES In the Crowd

### New VP at BAH

Booz Allen Hamilton, based in McLean, Va., appointed Keith R. Hall vice president. He is the former director of the National Reconnaissance Office and assistant secretary of the U.S. Air Force. As an officer in Booz Allen's national security practice, he will lead a strategic intelligence initiative to integrate activities across the firm's intelligence community clients.



*Keith R. Hall*

### Unisys Adds Two to Its Team



*Holli I. Ploog*

Unisys Corp., based in Blue Bell, Pa., hired Holli I. Ploog and Thomas M. Conaway for its global public sector team.

Ploog joins the company as vice president and managing principal of the global public sector programs. She is responsible for leveraging the company's portfolio of technology products, services and solutions to take Unisys to a position of market leadership in its key program areas, including justice and public safety; health and human services; administration and finance; and defense.

Conaway joins the team as managing principal, defense, global public sector. He will spearhead efforts to position Unisys as an end-to-end service provider to the Department of Defense and play a lead role in Unisys homeland security strategy.

### HP Picks John Hassell to Head Federal and State Government Programs

Hewlett-Packard Co., based in Palo Alto, Calif., named John Hassell, former HP public affairs director, head of the company's Washington, D.C., office and federal and state government affairs. He will manage HP's interactions with the U.S. Congress, state legislatures, the Bush Administration, governors and federal offices. He will also work closely with various companies, associations and coalitions on high-tech public policy issues and political activities.



*John Hassell*

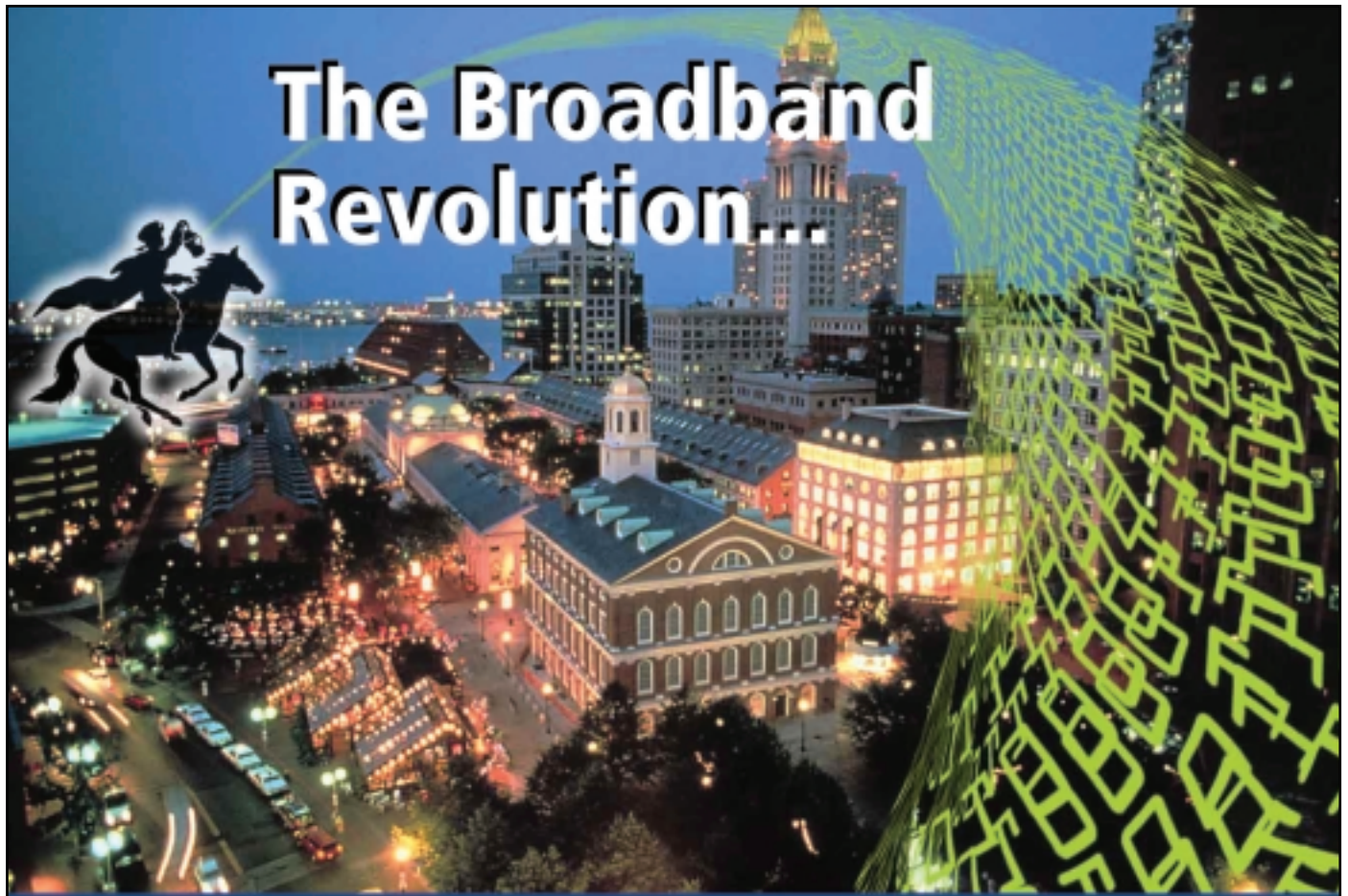
### Anteon Picks New VP/Treasurer



*Kelly R. Baker*

Fairfax, Va.-based Anteon International Corp. appointed Kelly R. Baker vice president and treasurer. Anteon is an information technology and systems engineering/integration company that has provided support to the U.S. federal government and international sectors for more than 25 years.

*Let us know about your organization's personnel changes. Send an e-mail to [faces@homelanddefense.com](mailto:faces@homelanddefense.com).*



# The Broadband Revolution...

## Wireless Leads The Way!

The 15th annual convention of the Wireless Communications Association

# WCA 2002

June 24-27, 2002  
Boston, MA, USA



### World Trade Center

- Benefit from presentations by 150 experts representing all BWA spectrum bands, US and international
- Review next generation products and services from the industry's leading equipment providers
- Network with top service providers and enterprise IT directors from 50 nations
- Attend special briefings on license exempt solutions, BWA in Latin America, WRC-2003, free space optics and homeland security

#### Sponsors

Diamond

**HARRIS**

Platinum

**NETRO**

Gold

**Sprint**

For information or to register:  
Wireless Communications Association International  
+1.202.452.7823 Tel • +1.202.452.0041 Fax • [colleen@wcai.com](mailto:colleen@wcai.com) • [www.wcai.com](http://www.wcai.com)



## State Security Initiatives Report

*Compiled by Stateside Associates*

Across the country, state governments are addressing homeland security. **Stateside Associates**, a national state and local government relations management firm based in Arlington, Va., compiled this roundup of recent state legislation and state executive actions aimed at combating terrorism.

### State Security Initiatives Overview

State legislatures are taking a measured approach in responding to security threats posed by the events of September 11 and its aftermath. Legislatures are not rushing to see how many bills they can pass. Instead, they are seeking to balance the need to protect the public from a terrorist threat with the need to protect individual liberties. Legislators across the nation are attempting to develop new emergency management, capital security and public health measures that are both fiscally sound and responsive to the needs and concerns of citizens.

Comprehensive initiatives have been proposed and enacted that make terrorism and the support of terrorism state crimes that can result in harsh punishment, including the death penalty. Since September 11, five states – New York, Florida, Virginia, South Dakota and Michigan – have passed initiatives that create crimes and penalties related to acts of terrorism. At least 15 states, including California and Minnesota, are still considering such criminal provisions.

Following September 11, states recognized the need to increase security to our nation's energy and water delivery systems. Several states have considered and passed legislation addressing threats to nature and our ecosystems. In Arizona, Arkansas, Connecticut, Kansas, Massachusetts, Missouri, New Jersey and New York, National Guard troops have been deployed to protect nuclear facilities. Additionally, Vermont and Massachusetts have offered legislative proposals to create a five-mile no-fly zone around their nuclear power plants.

A large number of health issues have come in to play as well, including bioterrorism, emergency health, workforce readiness, vaccines, rural health, and most prominently, the public health infrastructure. Health emergency legislation has been approved in Maryland, Maine, South Dakota, Utah and Virginia. Legislation is pending in more than 12 other states.

Legislatures have begun to enact safeguards against terrorist action in the areas of electronic surveillance and cyber-terrorism. Three states—Louisiana, Michigan and Virginia—enacted cyber-terrorism legislation because of September 11 events. Other cyber-terrorism legislation remains under consideration in California, Massachusetts, New York and South Carolina.

States	Issues
Alabama	No new action reported
Alaska	HB 350 Defines the crime of terroristic threat and provides a penalty
Arizona	HB 2044 Authorizes the governor to issue enhanced surveillance advisories, allowing the Department of Health Services and local health authorities to respond to public health emergencies by using enhanced reporting, isolation and quarantine measures*
Arkansas	No new action reported
California	AB 2099 Establishes a grant program for peace officer training in antiterrorism, and grants in support of acquiring necessary equipment to that end, as specified to be administered by the Department of Justice SB 1279 Enacts the California Antiterrorism Safety Bond Act of 2002, which, if adopted, would authorize, for the purpose of financing a program for antiterrorism safety, the issuance of bonds in an unspecified amount pursuant to the State General Obligation Bond Law
Colorado	HB 1315 - Declares that Colorado should establish an office to coordinate the state's response to terrorism, including the creation and implementation of terrorist preparedness plans
Connecticut	HB 5155 – Allows the commissioner of public health the authority to temporarily suspend licensure, certification or registration of certain public health professionals and provide such professionals immunity from liability during certain emergency situations*
Delaware	No new action reported
Florida	No new action reported
Georgia	No new action reported
Hawaii	No new action reported
Idaho	No new action reported
Illinois	No new action reported
Indiana	No new action reported

## Around The States

*continued from page 25*

States	Issues
Iowa	No new action reported
Kansas	No new action reported
Kentucky	No new action reported
Louisiana	No new action reported
Maine	No new action reported
Maryland	SB 1 False statements legislative branch units SB 20 Wiretapping police video*
Massachusetts	No new action reported
Michigan	SB 953 Amends Emergency Management Act to include procedures in cases of terrorism; adds category for local emergencies SB 1007 Requires financial institutions to seize funds of terrorist organizations and report to attorney general*
Minnesota	No new action reported
Mississippi	No new action reported
Missouri	No new action reported
Montana	No new action reported
Nebraska	No new action reported
Nevada	No new action reported
New Hampshire	HB1406 Permits the appointment of a temporary guardian for the children of activated members of the armed services and creates a committee to study the tuition waiver for national guard members*
New Jersey	AB 1764 Requires facilities that generate, store or handle certain explosives to comply with the provisions of the Toxic Catastrophe Prevention Act AB 1955 Appropriates federal funds for bioterrorism preparedness*
New Mexico	No new action reported
New York	SB 5808 Grants the governor certain powers when he or she determines that a state disaster emergency requires it SB 6161 Establishes procedures for convening a session of the state legislature by means of electronic video conference during a state disaster emergency in order to respond quickly and address the disaster
North Carolina	No new action reported
North Dakota	No new action reported
Ohio	SB173 Provides for the payment of specified compensation to certain public employees called to active duty for more than 31 days; requires public employers, under group policies, contracts and plans, to continue the health benefit coverage of employees called to active duty; and to declare an emergency.
Oklahoma	No new action reported
Oregon	No new action reported
Pennsylvania	HB 2149 Prohibits investments in countries identified as sponsors of terrorism. HR 374 Requires review of legislation and legislative recommendations on terrorism.
Rhode Island	HR 6657 Expands the Membership of the Special Legislative House Commission to study security issues at the state-house*
South Carolina	No new action reported
South Dakota	No new action reported
Tennessee	SB 2422 / HB 3109 - Allows home rule municipalities to collect actual administrative expenses incurred as result of false threat or hoax involving biological weapons, destructive devices, or weapons of mass destruction if such municipality has adopted ordinance to prohibit such threat or hoax
Texas	No new action reported
Utah	No new action reported
Vermont	No new action reported
Virginia	HB 58 Relates to an accessory after the fact of an act of terrorism is guilty of a class B felony SB 422 Creates criminal penalties for terrorism*
Washington	HB 2505 Creates penalties for training or teaching how to create a device or technique that causes injury or death to further a civil disorder*
West Virginia	No new action reported
Wisconsin	No new action reported
Wyoming	Gov. Jim Geringer (R) asked Attorney General Hoke MacMillan (R) to chair the state's new Counter Terrorism Council. The panel will evaluate the state's preparedness for a terrorist attack. The panel has yet to meet in 2002.

# Homeland Defense Business Opportunities

By Kelly Kingsley - Homeland Defense Journal

**Homeland Defense Journal** tapped into the database of its partner, Market\*Access International, to compile this list of homeland defense opportunities.

<b>Project</b>	Assessment of Counter-Terrorism Medications in Special Populations	Homeland Defense Contract to Design/Furnish/Install/Construct Security Systems	Joint Chemical Field Trials for Decontamination Devices/Technologies
<b>Department</b>	Program Support Center		Department of Defense
<b>Agency</b>	Transportation Security Administration	U.S. Army Corps of Engineers	Defense Threat Reduction Agency
<b>Summary</b>	<p>The Department of Health and Human Service's Program Support Center is soliciting proposals from the 14 National Centers of Excellence in Women's Health contractors to assess the changes in pharmacokinetics and pharmacodynamics of the prescription drugs used to treat medical conditions resulting from bioterrorist agents in:</p> <ul style="list-style-type: none"> <li>• Pregnant women during the second and third trimesters</li> <li>• Lactating women</li> <li>• Elderly women</li> </ul>	<p>The U.S. Army Corps of Engineers, Omaha District, is seeking sources and industry feedback for a homeland defense contract to design/furnish/install/construct security systems and related real property reinforcements within the Omaha district boundaries. The intent of this contract is to upgrade protection at government facilities including, but not limited to, dams, power plants, armories, reserve centers, military bases and government offices.</p>	<p>The Defense Threat Reduction Agency is sponsoring the Joint Chemical Field Trials-II (JCFT-II) as part of the Contamination Avoidance at Seaports of Debarkation Advanced Concept Technology Demonstration (ACTD). The JCFT-II will be used as the technical test bed to evaluate key performance parameters of selected technologies/devices for possible inclusion in the ACTD. Four commodity areas will be evaluated within the JCFT: detection, decontamination, personal/collective protection and medical.</p>
<b>Schedule</b>	RFP released July 2002 Proposals due August 2002	Sources sought notice released May 20, 2002	Information due June 14, 2002 Trials take place November 2002 to April 2003
<b>Value</b>		\$12 million	
<b>Contract Term</b>	24 months		
<b>Contract Type</b>			
<b>Agency Contact</b>	Marisha Foreman (301) 443-6762 mforeman@psc.gov	Tracey McKay (402) 221-4105 tracey.s.mckay@usace.army.mil	Jim Cannaliato james.cannaliato@sbccom.apgea.army.mil

*continued on page 28*

## Homeland Defense Business Opportunities

*continued from page 27*

<b>Project</b>	Optical Inserts for M45 CB Mask	Program and Integration Support Services Contract
<b>Department</b>	Department of Defense	Department of Defense
<b>Agency</b>	Rock Island Arsenal	Soldier and Biological Chemical Command
<b>Summary</b>	<p>The item to procure is an insert optical, or optical housing that will be used with the M45 chemical biological aviators mask. It provides a frame for vision corrective lenses for those personnel who require prescription lenses while wearing the mask. The item seats onto the mask main lenses from the inside of the mask. It consists of two lens frames made of nylon 12 material and connected in the center by a small titanium wire.</p>	<p>The U.S. Army Soldier Biological Chemical Command is issuing a solicitation to provide program and integration support services for its missions in research, development and acquisition, which includes developing, acquiring and sustaining soldier support, and nuclear, biological, and chemical defense technology, systems and services.</p>
<b>Schedule</b>	Responses due July 10, 2002	Request for proposals released June 28, 2002 Proposals due July 29, 2002
<b>Competition</b>	Small Business	Full and Open
<b>Contract Term</b>		Five years
<b>Contract Type</b>		Indefinite Quantity
<b>Agency Contact</b>	<p>Frances Taber (309) 782-3796 taberf@ria.army.mil</p>	<p>Tom Dickson (410) 436-8621 thomas.dickson@apgea.army.mil</p>
<b>Agency Web site</b>	<a href="https://aaais.ria.army.mil">https://aaais.ria.army.mil</a>	<a href="https://abop.monmouth.army.mil/ibophome.nsf/home">https://abop.monmouth.army.mil/ibophome.nsf/home</a>

Let us know about your company's recent contract awards. Send contract award announcements to **[wins@homelanddefensejournal.com](mailto:wins@homelanddefensejournal.com)**.

## Business Briefs

### *Anteon Corp. Wins Navy Contract*

Farifax, Va.- based Anteon International Corp., an information technology and systems engineering and integration company, won a contract amendment with an estimated value of \$10 million from the Naval Surface Warfare Center – Carderock Division. This latest award brings the total estimated value of this five-year contract, which lasts through December 2002, to \$49.5 million. The estimated value of the original contract was \$25 million. Under this contract, Anteon provides engineering, analytical, logistical and technical support services to the Carderock Division Surface Ships Engineering Station and combat support systems worldwide.

### *TRW Delivered*

TRW Inc., headquartered in Cleveland, delivered an advanced command and control operations center to the soldiers of the 263rd Army Air and Missile Defense Command Wednesday, May 22. The new operations center, called the Air and Missile Defense Planning and Control System, enables the South Carolina Army National Guard unit to deploy anywhere in the world to support theater air and missile defense missions.

### *Versar Supports First Responders*

Versar Inc., based in Springfield, Va., through its subsidiary, Geomet Technologies Inc., was awarded nearly \$1 million to provide specialized person-

al protective equipment to enhance the capability of federal, state and local levels of government to respond to weapons of mass destruction (WMD) and terrorist incidents involving the use of chemical, biological and radiological agents or devices.

### *Motorola Wins*

Fauquier County, Va., approved a \$7.2 million contract for a Motorola Inc. digital trunked wireless communications system. Under this contract, Schaumburg, Ill.- based Motorola would provide the system that enables county public safety agencies to communicate with each other over a shared system. It also would enable county agencies to communicate with many jurisdictions in adjoining counties that currently use similar systems.

*Let us know about your company's recent contract awards. Send contract award announcements to [wins@homelanddefensejournal.com](mailto:wins@homelanddefensejournal.com)*

## ANTI-TERRORISM AND HOMELAND SECURITY IMPLICATIONS FOR THE FY04 BUDGET

**June 4-5, 2002**  
**Regent University - Alexandria, VA**

This interactive, issue-oriented seminar will discuss the implications of 9-11 and offer solutions and strategies for preparing a compelling business case for FY04 funding.

#### *Featuring ...*

**Col. Randall Larsen** (USAF-Ret.), Director,  
ANSER Institute for Homeland Security (Non-Profit)  
**Robert Wilson**, Former Director, NSWC Innovation Center  
**Dr. Thomas Kessler**, Director, Denali Associates



For more info: 866-431-5005  
[www.denaliassociates.com](http://www.denaliassociates.com)

## ABOUT HOMELAND DEFENSE JOURNAL

Published twice monthly. Free to registered subscribers.  
Distributed as a PDF file and available for download.  
Printed version to be announced.  
Published by Homeland Defense Journal, Incorporated.  
Don Dickson, Publisher. Office:  
Homeland Defense Journal  
Suite 1003 4301 Wilson Boulevard  
Arlington, Virginia 22203  
[www.homelanddefensejournal.com](http://www.homelanddefensejournal.com)